The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
12/28/2009

SUBJECT:
Vulnerability in Microsoft IIS Could Lead to Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in Microsoft Internet Information Services (IIS) which is one of the most popular web servers in the world. This vulnerability exists on web sites where file upload is enabled. Successful exploitation could enable the attacker to bypass the file type filter and result in an attacker being able to upload a malicious file onto a vulnerable system. Depending on the privileges associated with the service, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

It should be noted that there is no patch available for this vulnerability.

SYSTEMS AFFECTED:

Microsoft IIS 6.0 and earlier versions

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: Low

DESCRIPTION:
A vulnerability has been discovered in Microsoft IIS which could allow an attacker to upload arbitrary files to an affected system. On web sites where file uploading is enabled, successful exploitation could enable the attacker to bypass the file type filter and result in an attacker being able to upload a malicious file onto a vulnerable system. This vulnerability is caused by the way IIS performs input validation on user-supplied filenames. Specifically, the server will allow the upload of a file with semi-colon characters after an executable extension such as ".asp".

Many web applications, particularly those which allow file uploads, only check the last portion of a filename as its extension. In an attack scenario in which the file "test.asp;.jpg" is uploaded to a web-server by an attacker, the server would accept the uploaded file as a harmless image. However, once the file is on the system, the server will render the file as an ASP page. If “Execute Scripts and Executables” permission is enabled for the site and depending on the privileges associated with the service, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

Remove "execute" permission from the IIS web directories where file upload is enabled.
Restrict file uploads to trusted users only.
Install the appropriate vendor patch as soon as it becomes available after appropriate testing.

REFERENCES:

Secunia:
http://secunia.com/advisories/37831/

Security Focus:
http://www.securityfocus.com/bid/37460

Vupen:
http://www.vupen.com/english/advisories/2009/3634

Microsoft:
http://blogs.technet.com/msrc/archive/2009/12/27/new-reports-of-a-vulnerability-in-iis.aspx

SANS:
http://isc.sans.org/diary.html?storyid=7810
http://isc.sans.org/diary.html?storyid=7816